

Memorandum

U.S. Department of Transportation
Federal Aviation Administration

Subject: ACTION: Electronic Controls Software Level for APU TSO Approval

Date: 7-28-97

From: Manager, Engine and Propeller Standards Staff, ANE-110

**Reply Mark
to Rumizen,
Attn. ANE-110:
of: (781) 238-7164**

To: Manager, Aircraft Engineering Division, AIR-100
Manager, Aircraft Manufacturing Division, AIR-200
Manager, Brussels Aircraft Certification Staff, AEU-100
Manager, Engine Certification Office, ANE-140
Manager, Engine Certification Branch, ANE-141
Manager, Engine Certification Branch, ANE-142
Manager, Boston Aircraft Certification Office, ANE-150
Manager, New York Aircraft Certification Office, ANE-170
Manager, Airframe and Propulsion Branch, ANE-171
Manager, Rotorcraft Directorate, ASW-100
Manager, Rotorcraft Standards Staff, ASW-110
Manager, Airplane Certification Office, ASW-150
Manager, Rotorcraft Certification Office, ASW-170
Manager, Special Certification Office, ASW-190
Manager, Small Airplane Directorate, ACE-100
Manager, Small Airplane Standards Office, ACE-110
Manager, Atlanta Aircraft Certification Office, ACE-115A
Manager, Propulsion Branch, ACE-140A
Manager, Chicago Aircraft Certification Office, ACE-115C
Manager, Propulsion Branch, ACE-118C
Manager, Wichita Aircraft Certification Office, ACE-115W
Manager, Propulsion Branch, ACE-140W
Manager, Anchorage Aircraft Certification Office, ACE-115N
Manager, Transport Airplane Directorate, ANM-100
Manager, Transport Standards Staff, ANM-110
Manager, Airframe and Propulsion Branch, ANM-112
Manager, Seattle Aircraft Certification Office, ANM-100S
Manager, Propulsion Branch, ANM-140S
Manager, Denver Aircraft Certification Office, ANM-100D
Manager, Los Angeles Aircraft Certification Office, ANM-100L
Manager, Propulsion Branch, ANM-140L

**Policy PS-ANE100-
No. 1997-00012**

1. INTRODUCTION

The Engine and Propeller Directorate was recently requested to provide written guidance regarding the minimum acceptable electronic control software level necessary for Auxiliary Power Unit (APU) Technical Standard Order (TSO) approval. This memo establishes a standardized policy for Aircraft Certification Offices (ACOs) to use when evaluating APU TSO programs.

The recent evolution of microprocessor technology in aerospace applications has resulted in the incorporation of electronic control units (ECUs) on APUs. These ECUs perform such functions as controlling fuel flow during starting, acceleration, and steady state conditions, preventing surge of the load compressor throughout the operating envelope, shutdown of the APU when hazardous conditions are indicated, and regulation of the APU air supply to the aircraft. These APU control functions are achieved through the use of sophisticated software imbedded in the ECU, and the validation and verification of this software is a significant element of the TSO design approval process.

The minimum performance standards which APUs must meet for FAA approval are defined in TSO-C77a. However, TSO-C77a was last updated in 1981, prior to the introduction of ECUs on APUs, and therefore does not address the use of computer software for APU control functions. This memo will provide specific guidance relative to the software requirements necessary for compliance with the FAA performance standard. These requirements should be conveyed to the applicant as early as possible in TSO process to allow ample opportunity for establishment of an acceptable software validation and verification program.

2. RECOMMENDED GUIDELINES FOR APU SOFTWARE CERTIFICATION

If the APU design incorporates a digital ECU, the imbedded software must be verified and validated in accordance with a methodology or guidelines that are acceptable to the FAA. The FAA has determined that the software verification and validation methodology specified in RTCA Document No. DO-178B, "Software Considerations in Airborne Systems and Equipment Certification", dated December 1, 1992, is an acceptable means of software validation and verification. The DO-178B methodology establishes software verification and validation requirements based on the level of software integrity necessary for safe operation, as determined by the contribution of the software to potential failure conditions. Therefore, for those applicants who elect to use RTCA Document No. DO-178B to demonstrate compliance of the ECU software with FAA TSO requirements, the failure condition categorization and associated software level must be determined in accordance with the following:

a. Failure Condition Categorization

APU ECUs control critical operating parameters such as fuel flow and the speed of high energy rotating components. Software errors can produce failure conditions that are potentially hazardous to the aircraft and passengers such as overspeed or fuel flow scheduling errors that lead to uncontained failures or fires. Categories that have been established to characterize the severity of these failure conditions are described in section 2.2.1 of DO-178B. A safety assessment analysis should be performed by the APU manufacturer to assess the contribution of the ECU software to potential APU failure conditions and to specify the associated failure condition category. However, because the software failure contribution level should be consistent with the complexity and inherent hazards of these fuel-fed, high energy gas turbines, the

“Major” failure condition category, as defined in DO-178B, section 2.2.1, c, is considered the minimum acceptable level. Failure condition categories of “Hazardous/Severe-Major” or “Catastrophic”, which represent more severe levels of failure contribution, may also be applicable, depending on the results of the system safety assessment. However, the applicant should be cautioned that system safety assessments that result in minimum acceptable failure condition categories of “Major”, could be incompatible with some aircraft installations that are less tolerant of APU failures than assumed during the safety assessment process. In this case, installation of the APU could not be approved until either the APU software is requalified to the more severe failure condition categories or the fault tolerance of the aircraft installation is improved.

b. Minimum Acceptable Software Level

Once the contribution of the software to potential failure conditions is determined in terms of the Failure Condition Category, the software design assurance level necessary to ensure safe operation can be defined. The software level will dictate the scope of the verification and validation requirements from DO-178B. As discussed above, the minimum acceptable failure condition category is “Major”, and therefore, the minimum acceptable software level is Level C, in accordance with DO-178B, section 2.2.2, c. Furthermore, depending on the results of the system safety assessment, software Level A or B, which are associated with the more severe failure condition categories and which specify more rigorous verification and validation criteria, may be required. The applicant should be advised that TSO approval to the minimum acceptable level of C could be inadequate for the intended aircraft installation requirements of FAR 25, and the software may require recertification to a higher level.

All ACOs should ensure that applicants seeking TSO approval for APUs equipped with ECUs substantiate that the imbedded software meets the criteria of DO-178B software Level C, as a minimum. However, a DO-178B Software Level A or B may be required, depending on the results of the system safety assessment.

Original Signed By:
Thomas A. Boudreau